JÓZSEF HAJDÚ[+]

The protection of employee's privacy in Hungary, with special attention to data protection

„Aogeba totoshi, Wagashino on"
(Whenever I look back the way I come along, I find my senior's warm and attentive eyes.)

Introduction

One of the most important and most frequent scenes of human connections is the workplace. The danger of infringing personality rights is more pronounced here. In Hungary – especially after the change of the regime – the employees' subordinate situation, their state of being uninformed, lack of consciousness and also data collection and data processing made possible by technical development all contributed to the continuous endangering of the employees' personality rights.

Since the beginning of the 90s the employees' dependence on the labour market and their defenselessness have been increasing in Hungary. One can observe the continuous erosion of previously obtained – although sometimes no more meaningful – employees' rights, worse enforceability and the pushing of interest representation in the workplace into the background. The preponderance of the power of information on the employer's side, the frequently unfavourable, unequal communication on the employee's side infringe the fundamental personal rights and the right to privacy.

[+] Associate professor (Department of Labour Law and Social Security, Faculty of Law at Szeged University, Szeged, Hungary)

Employers collect personal data on job applicants and workers for a number of purposes: *a)* to comply with law; *b)* to assist in selection for employment, training and promotion; *c)* to ensure personal safety, personal security and the protection of property.

New ways of collecting and processing personal data, made possible by advances in information technology, entail some new risks for workers. As enterprise operations become more global, data transfers across borders make the protection of personal data more complex.

Taking into consideration of the international and EU trends, the first part of the paper gives a survey of the general rules of the Hungarian data protection legislation.

In the second part, a substance is given to the right of privacy of the worker during the employment relationship. In this part the background of employee's privacy legislation and some cases from the practice of the Hungarian Data Protection Commissioner will be introduced.

I. General rules of the Hungarian data protection legislation

1. Historical background

The legislation and application of law on *data protection* and on the *freedom of information* date back to a relatively short past, but due to the legal vacuum arising as a result of the appearance of computer registers their regulation, especially that of data protection, was very rapid. In our days the technical possibility of data storage and data transfer has increased drastically as computers have become widely used and have seen a rapid development. A great number of registers have been made about natural persons and legal entities, and during the handling of these data personality rights must be respected. This can be endangered if the register contains untrue, faulty, out-of-date or confidential data, and due to the large-scale use of data registers this danger is not negligible. The technical possibility of connecting individual data bases may also be dangerous as it can happen without the person's knowledge and consent, thus he or she cannot influence it.

In spite of the fact that in Hungary the issue of data protection and freedom of information was hardly known in the past, the necessity of their regulation was pointed out as early as at the beginning of the 80s. This procedure was accelerated by Act XXXI of 1989 on the amendment of the Constitution, which was the first in Central Eastern Europe to raise these two rights to the constitutional level, thereby adding them to the chapter on fundamental rights and obligations. Finally, *Act LXIII of 1992 on the Protection of personal data and disclosure of data of public interest* was passed by Parliament in October, 1992.

As concerns Hungarian data protection, in 2000 the European Union (EU) stated that its level corresponded to the relevant Directive on Data Protection of the EU.[1] In an international comparison the Act reflects the way of thinking about data protection in Europe at the beginning of the 90s. Its specificity lies in the fact that in contrast with its generally used title it is not a "data protection" act but the act of information freedom rights: in addition to the protection of personal data, the guarantees of the freedom of information are also regulated, and these two freedom rights are entrusted to a common protector, to the Commissioner for Data Protection and Freedom of Information. This dual role continuously urges the commissioner to try to find the middle course between these two freedom rights, which often seem to be in contradiction and which mutually restrict each other.

2. Data protection in civil law

Data protection protects the individual from the unlawful use of information obtained by processing facts concerning the individual. In this respect the greatest threat is posed by electronic data procession.

One may institute court proceedings against the data controller handling *personal data* illegitimately. In the lawsuit compensation for possibly arising damage – both pecuniary and non-pecuniary – can be claimed. The latter one can be claimed in case the human personality's physical or mental life quality has changed unfavourably in consequence of the violation of personality rights. The court in the place of the controller's business shall have jurisdiction over the case.

In addition to this method of assertion of right, the data protection commissioner's help may also be requested.

According to Paragraph (1) of Article 83 of the Civil Code: *"Data handling and data processing with a computer or in other ways may not violate personality rights.*

(2) Information about the data on register can be given – apart from the person concerned – only to an organ or person entitled to it.

(3) If some facts or data in the registers are untrue, the person concerned may demand the correction of the untrue fact or data in the manner regulated in a special rule of law."

§ 3 of the Civil Code: A legal rule may prescribe that the court procedure aimed at correcting the computerised register has to be preceded by a state

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

See.: http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm.

administrative procedure. In the absence of such a regulation the party can go directly to court.

The act provides protection mainly for persons in the register. The protection is two-directional: *a)* on the one hand no information can be given about the registered, processed data to unauthorised persons; *b)* on the other hand the correction of untrue data and facts can be requested. The special emphasis on the rules pertaining to computerised registers and data processing does not mean that protection is restricted to this field. In certain cases the infringement of personal rights can arise in the course of data registering and processing with some other method, and the proper means of protection are available in those cases, too.

3. Means of data protection in criminal law

The importance of questions of data protection is indicated by the fact that the state ordains that certain acts committed at the expense of data subjects be punished. These repressive sanctions have been formulated by the legislators in the form of misdemeanour or criminal law facts. These are the following: *a)* misdemeanour concerning data protection,[2] *b)* unauthorised data handling,[3] *c)* abuse of special personal data[4] and *d)* computer fraud.[5]

4. The principles of data protection

4.1. Right of informational self-determination

In accordance with the spirit of the age, data protection is worded as a positive freedom with increasing frequency, called a right of informational self-determination, it is not interpreted as a traditional protection right but its active

[2] Government Decree 218/1999 (XII. 28.) on misdemeanour.

[3] Hungarian Criminal Code Art. 177/A. "The person handling data, who a) handles personal data illegitimately or diverting from its purpose; b) forwards or publishes personal data illegitimately; c) fails to fulfil his reporting obligation relating to the handling of personal data; d) conceals personal data from a party entitled thereto; e) falsifies personal data handled; f) conceals or falsifies data of public concern commits a misdemeanour (...)"

[4] Hungarian Criminal Code Art. 177/B. „The person who a) illegitimately publishes; b) uses illegitimately or makes available to an unauthorized person the special data learned by him in the course of his data handling defined in the legal rule relating to the protection of personal data, commits a felony (...)."

(2) The person who illegitimately obtains special data for himself or somebody else, commits a misdemeanour (...)."

[5] Paragraph (1) of § 300/C of the Criminal Code: "The person who alters the results of electronic data processing by changing the program, by deletion, by entering false or incomplete data or by performing some other, illicit operations for the purpose of gaining illegitimate benefits or causing damage thereby commits a crime (...)."

aspect is pointed out. This is also confirmed by the relevant resolution of the Constitutional Court,[6] which interpreted the protection of personal data provided for in § 59 of the Constitution[7] as a right of informational self-determination and stated that according to the content of this right each person is entitled to exercise control over the disclosure and use of his or her private secrets and personal data. In another resolution[8] the Constitutional court expounded the content of this: "each person exercises control over the disclosure and use of his or her personal data. Therefore personal data can generally be registered or used only with the consent of the person concerned; the whole procedure of data processing should be traceable and controllable by everybody, in other words everybody is entitled to know who uses his or her personal data and where, when and for what purpose. An act may exceptionally prescribe the obligatory provision of personal data and may also prescribe the manner of its use."

4.2. Specified purpose (purposefulness)

The condition and at the same time the most important guarantee of exercising the right of informational self-determination is the specified purpose, which means that personal data can be processed only for specified and lawful purposes. The person concerned has to be informed about the aim of data processing in such a way that he or she will be able to judge the effect of data processing on his or her rights and to make a well-founded decision about the disclosure of the data; furthermore he or she has to be able to exercise his or her rights in the case of using the data for another purpose.

4.3. Prohibition of data processing for stock

It ensues from the nature of specified purpose that data collection and storage "for stock", without a specified purpose, for a future use not yet defined is against the law.

4.4. Restriction of data transfer and disclosure

In a stricter sense data transfer is the operation during which the data are made available by the data processor to a certain third person. Disclosure means that any third person can have access to the data. In accordance with the act

[6] 20/1990 (X.4.) Resolution of the Constitutional Court.

[7] Paragraph (1) of Article 59: „In the Republic of Hungary everyone has the right (...) to the protection of personal data. (2) A majority of two-thirds of the votes of the Members of Parliament present is required to pass the law on the secrecy of personal data."

[8] 15/1991 (IV.13.) Resolution of the Constitutional Court.

personal data can be made available to a third person, apart from the person concerned and the data processor, – in this way connecting data processing systems – only if all the conditions of data transfer have been fulfilled with regard to each piece of data.

5. Basic characteristics of the Hungarian data protection act

In Hungary data protection is regulated not only by the Civil Code but also by the Act on Data Protection.[9] The act makes a distinction between personal data and special data.

The act defines the concept of personal data as follows: *"personal data means any data relating to a specified natural person (hereinafter called data subject) and any conclusion drawn from such data with respect to him or her. As long as the data subject can be identified by the data, it preserves this personal characteristic"*[10] Thus personal data are conclusions drawn concerning the person (e.g. ability to fulfil a post, credit-worthiness, workplace promotion,); that is all information about an identified or identifiable person. Pursuant to the act *special categories of data mean any personal data relating to a) racial origin, nationality, national or ethnic origin, political opinion or party affiliation, religious or other belief, b) health, pathological addiction, sexual life and criminal conviction."*[11]

Based on international practice, these special data are also given increased statutory protection in Hungarian law. In accordance with this the handling of special – so-called sensitive – data can be ordained or permitted only by an act, or the expressed, written consent of the person concerned is necessary.

[9] Act LXIII of 1992 on Data Protection.

[10] Paragraph (1) of Article 2 of the Act on Data Protection.

[11] Paragraph (2) of Article 2 of the Act on Data Protection.

5.1. Data controller – data processor[12]

Data controlling encompasses all possible operations applied to data. However, as the activity is defined, the regulations applied need not be described. All the listed data-controlling activities are not necessarily performed by the same person, but data controlling has to meet statutory requirements in all phases. If for any reasons – for example cost saving – data are registered not with the direct participation of the person concerned but by means of data transfer, the other provisions of the act on data protection have to be applied all the same, and the consent of the person concerned has to be obtained either at the time of data registering or before transfer.

The 1999 amendment of the Act on Data Protection made up for one of the greatest deficiencies of the Hungarian legal regulation,[13] as it made a distinction between the data controller and the data processor. This distinction, also applied by the Data Protection Directive of the EU, was justified as it is required by law that the data controller with its own responsibility can employ a participant for whose activity the data controller takes legal (naturally, mainly civil law) responsibility.

Based on the Data Protection Directive, the data processor is under the legal obligation to process the data only in accordance with the instructions of the data controller, meeting the requirements of data safety. Derogation from this principle is possible only in case of statutory authorisation.[14]

Thus civil law responsibility becomes clear: the data controller is responsible for his or her own instructions and also for choosing the data processor with due care; the civil law responsibility of the data processor can also be ascertained, especially if he or she departs from the data controller's instructions. However, the possibility of ascertaining the criminal law responsibility of the data processor, especially with respect to the criminal law

---

[12] Point b) of Paragraph (4) of Article 2 of the Act on Data Protection: "technical data processing means any operation and technical activity performed upon personal data, irrespective of the method and means employed, as well as of the place of operation"

Paragraph (2) 4/A. "The data processor is responsible for the processing, alteration, deletion, transfer and disclosure of personal data within his or her competence and under the instruction of the data controller. During this activity the data processor shall not entrust other processors."

Paragraph (2) of Article 6: "The data subject shall be informed of the purpose of processing, as well as of the controllers and processors. The communication on data processing can also be accomplished by law providing for the collection of data from an existing file by way of transfer and file connection." Pursuant to Point a) of Paragraph 4 of the Act *data controlling* is: "the collection, registering, storing, processing, use (including transfer and disclosure) and deletion of personal data, irrespective of the procedure used. The alteration and the prevention of the further use of data also qualify as data controlling."

[13] Act LXXII of 1999 on the amendment of certain acts related to the handling of the personal data of citizens.

[14] Article 16 of 95/46/EC.

facts of unauthorised data handling and abuse of special personal data (§ 177/A, § 177/B of the Criminal Code)[15] raises further dogmatic difficulties due to the personal nature of criminal law responsibility.

5.2. Data transfer, disclosure of data[16]

In a stricter sense data transfer is the operation during which the data are made available by the data processor to a certain third person. Disclosure means that anybody can have access to the data. Data transfer makes the personal data available to certain defined person(s); on the other hand, in the case of disclosure anybody can have access to them. The person who carries out the physical of computer tasks of data processing for and charged by the data controller – usually in a professional or business-like manner – is not considered to be a "data processor", and making the data available to this person does not qualify as "data transfer". The responsibility of such a charged person is to be regulated separately, leaving the data processor's full responsibility for data transfer performed both by himself/herself or by another person untouched.

5.3. Connecting of data control[17]

Personal data can be made available to a third party, apart from the person concerned and the original data processor, – and thereby data processing systems can be connected – only if all the conditions of data transfer are fulfilled with regard to each piece of data. The addressee of the data transfer (person requesting the data) either has to be in possession of a concrete statutory authorisation in order to be allowed to process the transferred data or he or she has to have the consent of the person concerned. Naturally, specified purpose is the greatest obstacle to transfer.

The data controller transferring the data is obliged to check the conditions of data transfer and connection as he or she is responsible for the personal data handled by him or her, and the data controller is obliged to inform the person concerned to whom and for what purpose his or her personal data were or will be transferred.

---

[15] For more details see point III/8.

[16] Paragraph (5) of Article 2 of the Act on Data Protection: Data transfer "means access by specified third person to data" (6) Disclosure "means access by anyone to data."

[17] Paragraph (1) of Article 8 of the Act on Data Protection: Data shall not be transferred and files shall not be connected unless consented to by data subject or provided for by law. The conditions for data processing shall be met in each case with regard to each personal data.

(2) Connection of files processed by the same controller, as well as those of state organization and self-governments shall likewise be governed as in para (1).

Data security is one of the institutional guarantees preventing unauthorised access to and use of personal data. It gives the possibility to the data controller to decide, in view of the location and means of data handling and the methods of possible traditional and electronic access, to take specific measures of security, at the same time it also increases his or her responsibility because if the protection used proves to be insufficient, his or her civil law and criminal law responsibility still exists.

The right of informational self-determination can be exercised if *data registering* is made from the person concerned and with his or her knowledge. Possible other variations of these two conditions – with or without his or her knowledge but from somebody else, or without his or her knowledge but about or from him or her (e.g. with secret observation, tapping) – endanger the personality rights of the person concerned to an inadmissible extent. Such data registerings can be made only in certain cases strictly defined by law. Knowledge is not equivalent to consent, and especially not equivalent to informed consent. Therefore, irrespective of whether data supply is voluntary or compulsory, the concerned person can make a well-founded decision only if he or she is aware of the consequences of refusing data supply. This is the reason why the rule of law pertaining to data supply has to be indicated as well as the purpose of data handling and the person of the data controller. The compulsory elucidation of the consequences, purposes and entitlements refrain from unlawful claims.

For reasonable causes – saving of costs, relieving of the person concerned – data may not always be registered from the person concerned. However, he or she has to have the right to know who handles his or her data, where and for what purpose, from what source they were obtained, and he or she also has to be able to make certain his or her data are correct and that data handling is lawful. The declaration of these rights constitutes one of the guarantees of the lawfulness of data handling. It is more expedient to regulate other guarantee rights as the data controller's obligations.

6. Data protection self-regulation

Data protection self-regulation means the independent systems of rules of professions, associations, corporations, chambers, societies and business sectors, with the consideration of state law.

The main structural weakness of the Hungarian data protection law possibly lies in the disorder of self-regulation, even though it is one of the most important fields of data protection in everyday legal life and right assertion. The Netherlands is usually quoted as an example, where the self-regulating activity of data controllers is made the statutory part of data protection by the act on data protection, what is more, light statutory regulations are levelled by

the strict sectoral self-regulating mechanisms. Self-regulation makes the development of data protection more lively and organic.

Self-regulation is treated by the EU Data Protection Directive as an important part of national and European systems of data protection: "The member states and the Commission encourage the formulation of ethical regulations which – with the consideration of the specific nature of individual sectors – promote the proper application of internal regulations made in correspondence with the Directive."[18] The Directive gives not only encouragement but it also advises professional associations, data controllers to present their regulations to the data protection authority in order to check whether they correspond to the state data protection law, and as such, to the Directive. Self-regulation is the field in which the Hungarian data protection law undoubtedly falls behind the European Union average – although in the internal regulations of some direct marketing companies, some chambers and the Association of Hungarian Journalists positive examples can be seen.

7. Parliamentary Commissioner for Data Protection and Freedom of Information Hungary

The establishing of the position of the Parliamentary Commissioner for Data Protection and Freedom of Information was ordained basically by the 1993 Law on the Parliamentary Commissioners, however, in the case of the Data Protection Commissioner (also known as the Data Ombudsman), already the Data Protection and Freedom of Information Law of 1992.

The integration of tasks and functions of the Data Protection Commissioner constitutes a unique solution. Besides monitoring both data protection and freedom of information in general with an ombudsman-like competence, the Commissioner's tasks are many-sided. They include the maintenance of the Data Protection Register, the giving of opinion on DP and FOI-related draft legislation as well as each categories of official secrets; and, according to the Secrecy Law of 1995, the Commissioner is entitled to change the classification of state and official secrets as well.

Anybody can initiate the intervention of the data protection commissioner in his or her own case. A general announcement can also be made for example against the unlawful practice of a certain data controller. If the data protection commissioner ascertains unlawful data handling, he or she will order the data controller to cease data handling. The data controller is obliged to take the necessary measures without delay, about which the commissioner shall be informed within thirty days. Naturally, he or she is entitled to make a criminal report, too.

[18] § 27 of 95/45/EC

It ensues from the rights of the data protection commissioner that no data handling, personal or public data can be kept secret in his or her field of activity.[19]

8. Data protection registers

The data protection register is very special; it is kept by the office of the data protection commissioner. On the one hand, the data protection register serves the purpose of checking the lawfulness of data handling, and on the other hand it makes it possible for the person concerned to learn about the handling of his or her data, especially if he or she cannot exercise his or her right of informational self-determination directly. Thus the purpose and significance of the registers is that citizens can check who handles what personal data, in which registers they appear. It follows from this that, interestingly enough, the data protection register does not contain personal data as it is a register of registers.

Each data controller is obliged to report to the data protection commissioner before starting his or her activity.[20]

II. Protection of personality rights in labour law

1. Introductory remarks

1.1. The trends of the employment related data protection cases

In developed, democratic countries the data controller-data subject relationship between employers and employees is a classical field of data protection. Although Hungary is familiar with the international practice as well as with the relevant international documents, Hungarian sectoral legislation on data protection has not paid due attention to the regulation of this field yet. Moreover, the employees' attention, consciousness, sense of danger and especially their willingness to take action against infringement of their rights fall much behind other fields of labour law.

Even so, the number of complaints associated with data handling by the employers has increased for the last few years, which indicates that data handling related to the legal relationship aimed at performing work is becoming a more "sensitive" area in data protection. One possible explanation for this is that the major element of the content of the right of informational self-determination, the voluntary nature of the consent to data handling – as

[19] http://www.obh.hu/adatved/indexek/index.htm

[20] http://www.obh.hu/adatved/indexek/index.htm

employees are under pressure because of their financial vulnerability – cannot be determined in many cases. However, some of the employers are willing to act in a lawful manner, which is indicated by the fact that they often hand in consultation petitions to the office of the data protection commissioner before taking measures concerning the data handling of employees.

The year of 1997 saw a rise of complaints against employers, both in terms of number and significance. With respect to their substance, these cases concern three basic issues: *a)* At hiring and during the term of employment, what type of personal and sensitive data may the employer request from the employee or collect about him? *b)* To what extent and how can employees avail themselves of the right to access their own personal data in the files kept by the employer? *c)* In what cases and conditions may the personal data of the employee be forwarded to a third party or be disclosed to the public?

The single most important development in 1999 was the moderated rise in the number of complaints against business organisations.

In 2000 the number of the data protection related cases were again on the rise, after a tendency of moderate rise over the period of 1998–1999. However, it wasn't a dramatic change. Fewer large data controllers, private or public, seemed to risk a plunge in the dark on the basis of *"Let's see if we can get away with this."* They tended to be more careful in preparing programs involving or targeting the processing of personal data, and to choose the lesser of two "business evils" by contacting the Office of the Data Protection Commissioner with requests for advice. More and more companies find that it will be worth their while to incorporate data protection considerations into their business plans, on the principle of a cost/benefit analysis.

Undeniably, the picture was and still is less bright in the area of freedom of information. While there were no significant changes in the ratio of data protection and freedom of information cases, the latter never accounted for more than 8 or 9 percent in any cluster of cases isolated by various criteria. The groups and persons raising a voice for freedom of information can be predictably identified as journalists, politicians (typically of an opposition party), and environmentalists. The involvement of society at large falls behind both international standards and what the conditions would permit in Hungary.

The bottom line was to develop the area of freedom of information. Those who have enlisted in the fight to protect informational liberties must become used to the idea that the information industry, as it makes inroads in both private business and public administration, is not only unstoppable but also bent, by its very nature, on disregarding the interests of privacy. In Hungary as elsewhere in the world, new tools are invented daily that assist in the assault upon the increasingly helpless individual, in the invasion of privacy. The forces of data protection are often relegated merely to slowing down this harmful process, incorporating guarantees in the system against it, and to promote awareness of the danger – all essentially forms of backing down.

It could be enlisted the assistance of legal solutions and privacy-friendly technologies already adopted abroad. In contrast to these options, the past year appeared in Hungary as well, such as privately-controlled biometric identifiers, lie detectors, devices to analyse the human voice, genetic maps, etc. Presumably, we will not have to wait long for the introduction of heat-sensitive cameras that can see through walls. Everyone can imagine the results.

2001 showed no sign that complaints against employers were down. The large number of petitions from employees is rooted not only in their existentially vulnerable position, but also in the simple fact that the majority of people are engaged in some kind of employment relation or other.

The previous tendency of the increasing number of petitions concerning data controlling by the employers changed. In 2002 the number of complaints and requests for consultation was smaller than in previous years.

1.2. Legal basis of the Hungarian employees' personality rights

The data controller/data subject relationship obtaining between employers and employees is a traditional area of data protection in advanced democracies. Even though the international policies are known in Hungary, as are the related international legal norms (e.g. the 1989 recommendation of the Council of Europe on the Protection of Personal Data in Employment), data protection legislation in Hungary has not paid sufficient attention to this area to date. Furthermore, employees in the past tended to be far less aware, self-conscious and not especially willing to stand up against violations than in other contexts. The number of complaints against employers and places of employment was not very high. One reason for this could be the vulnerable situation of those seeking work. Employers often force workers to fill out questionnaires and data sheets which gravely violate individual rights.

In case of the infringement of personality rights during performing work the Civil Code (general rule) has to be used as a background legal rule because the Labour Code[21] (special rule) does not declare the full-scope protection of the person while it contains provisions of such nature. On the one hand, in accordance with § 76 of the Civil Code, Paragraph (1) of § 5 of the Labour Code prohibits discrimination from all aspects not related to the employment relationship: „In connection with employment relationship, no employee shall be discriminated against according to sex, age, family status or handicapped state, nationality, race, origin, religion, political beliefs, affiliation with employees' interest representation organisations, their activities related to this and any other circumstance not related to employment relationship."

On the other hand, the employer's behaviour infringing personality rights may be prohibited by the unlawful exercise of rights incorporated in § 4 of the

[21] Act XXII of 1992 on the Labour Code.

Labour Code. In this respect infringement of rights is most often encountered when the employer exercises its rights related to the employee's supervision and instruction in an abusive manner offending the employee's person.

A major part of complaints is associated with the protection of the data of persons applying for a certain post, before the legal relationship aimed at performing work is established. The most frequently arising questions are the following: what personal data may an employer ask from its would-be employee, under what circumstances they have to be stored and what will happen to the registered personal data.

Apart from the basic principles, some articles of the Labour Code deal with the protection of the employees' personality rights. With respect to the dynamics of employment relationship, four different phases should be distinguished from the viewpoint of employee protection: *a)* Period of establishing employment relationship and preceding talks; *b*) Existence of the employment relationship; *c)* Handling and protection of personal data concerning the employee and registered by the employer, and *d)* Responsibilities after the termination of the employment relationship. These points will be dealt with from a practical point of view in the following pages.

2. Protection of personality rights during the establishment of employment relationship and preceding talks

As concerns the first question, § 77 of the Labour Code ordains: *"The employee may be requested to make a statement or to fill in a data sheet, or may be subjected to an aptitude test which does not infringe his or her personality rights and which may give important information with respect to establishing the employment relationship."*

The Labour Code is extremely brief about the range of data which can be registered by the employer, it only prescribes that the employee may be requested by the employer to fill in a data sheet or may be subjected to an aptitude test which does not infringe his or her personality rights and which may give important information with respect to establishing the employment relationship, and the act also gives authorisation for the handling of data related to working hours and days off. In the labour contract natural personal identification data (name, mother's name, place and date of birth, address) necessary for identifying the employee are to be included as appropriate. Other acts ordain that the employer is obliged to handle certain personal data, for example the employer has to register the employee's tax number and social security number as these are necessary for fulfilling its tax return and other payment obligations. There are employers – especially in the public sphere – for which the relevant acts prescribe concretely what data may and have to be registered about their employees. The employer is not allowed to oblige the employee to supply data for the handling of which it has no statutory

authorisation, thus for example the employee's personal identification number cannot generally be handled by the employer.

Many employers would like to know as much about their employees as possible, what they do in their working hours and in their free time, who they maintain relationships with, what they use the infrastructure of the workplace for. The employees are watched through cameras, their correspondence is checked, their phone calls are listed, their e-mail and internet use is monitored. This cannot be done without restrictions.

Thus the employee does not have to answer questions not related to the post to be taken. If the employer refrains from establishing employment relationship on account of refusing the answer to the question, this may mean the infringement of the would-be employee's personality rights, thus the would-be employee can enforce his or her claim in court. According to the Code of Civil Procedure, these legal disputes belong to the competence of the labour court in spite of the fact that no employment relationship has been established between the parties yet.[22]

In practice the problem outlined here arises mainly theoretically. The reason for this is that in the present labour market situation the employee is hardly likely to openly refuse to answer questions infringing personality rights during the interview as in this case his or her application may possibly be rejected. Assertion of right in court is very rare in connection with this, although the theoretical possibility undoubtedly exists. The problem could be solved by making the statutory regulation more exact by specifying the data relevant to employment relationship and by determining the legal guarantees of the procedure. Such a guarantee could be, for example, the written registering of the interview, the registration of questionnaires and tests and their handing out to the applicant, the previous professional authorisation of psychological and personality examinations not subject to various legal regulations, the prescription of the requirements necessary for taking the post in the employer's internal regulation, etc.

The other typical form of right infringement during establishing an employment relationship is discrimination among employees on the basis of impermissible considerations, which violates the already mentioned § 5 of the Labour Code. /In fact the above case can also be regarded as discrimination, that is if the employer forms an employment relationship with the employee who is willing to answer the unlawful questions./

It is not always easy to decide whether the information requested by the employer or the circumstance on which the selection was based is related to the employment relationship as due to the contractual freedom the employer is entitled to decide the other viewpoints, in addition to the criteria closely connected to the nature of the job – such as qualification, experience, etc. – on

[22] Act III of 1952 (Code of Civil Procedure) Point a) of Paragraph (2) of Article 349.

the basis of which the applicant is selected. It is always decided by the circumstances of the given case whether discrimination is lawful or not. Accordingly, the employer is entitled to choose an employee with lower qualifications instead of the higher-qualified employee if this is justified by some other circumstance connected to the employment relationship. Paragraph (5) of § 5 of the Labour Code: *„Distinction evidently ensuing from the nature or type of work does not qualify as discrimination."*

Paragraph (8) of § 5 of the Labour Code adds another essential rule – exculpatory evidence –: *"In case a dispute arises in connection with the employer's procedure, the employer is to prove that the regulations concerning the prohibition of discrimination were not violated."*

2.1. Problems associated with the establishment of employment relationship on the basis of cases from the practice of the data protection commissioner

a) A question arising in each year is what the employer has to do if the application of a person to fulfil a job is rejected. In the hope of finding employment, applicants are willing to supply almost any personal data, but after being rejected they object to their data being handled by the organization which chose not to employ them. In one case the applicants changed his mind a few hours after the job interview and did not wish to apply for the job any more, so he asked to be given the registers containing his personal data, made during the interview, but his request was rejected. On being questioned by the commissioner, the legal representative of the company claimed that the sheet of the paper containing the personal data could not be returned to the applicant as it also contained the data of other applicants. Later the request of the applicant for the deletion of his data was fulfilled by destroying all the registers made about him. The legal representative of the company also informed the commissioner about the purpose of data registering: it was made in case another interview was held or for subsequently concluding a labour contract. The data protection commissioner pointed out to the representative of the company that certain personal data requested during the interview – in connection with financial situation and housing circumstances – were in conflict with the principle of specified purpose. The commissioner informed the applicant that the supply of data was voluntary, thus in a similar situation he was entitled to refuse to give the data. (828/A/1999)

In my view it is true that the supplying of data is voluntary and the applicant can decide whether to answer all the questions, but the employer violated § 77 of the Labour Code even by posing the question, as questions concerning financial situation and housing circumstances do not qualify as information essential with respect to employment relationship, and as such, they infringe personality rights.

The employers have the right to employ persons for certain posts who, on the one hand, have the necessary qualifications, on the other hand – if the job in question is confidential and entails great responsibility – have a background which excludes or at least reduces potential risk factors. Thus the employers may require several personal data when the employees are chosen. The act does not specify the data which can be handled by the employers, but the above-quoted regulation of the Labour Code delimits data handling in harmony with the principle of specified purpose defined in the act on data protection.

b) In other case the lawyer of a department store chain asked the Data Commissioner's opinion about what should happen to the personal data after the job interview if no employment relationship is established. According to the requirement of specified purpose, the data of unsuccessful applicants are deleted after the application procedure, but in this way they cannot inform the person concerned, in accordance with § 12 of the Act on Data Protection, of data controlling, and in case of possible complaints of discrimination they cannot give reasons for the refusal. The Data Commissioner stated that after the deletion of personal data the data controller ceases to be a data controller thus pursuant to § 12 of the Act on Data Protection – if he or she did not transfer the personal data previously to a third person – he or she is not obliged to give information to the person concerned, and upon being asked he or she has to answer that he or she does not handle data concerning the person. If, however, data transfer was made, the person concerned has to be informed about the registered data of data transfer (to whom and for what purpose personal data were transferred) as this register is not to be deleted together with the personal data supplied during the interview. Furthermore, it was pointed out that in the case of hiring workforce the personal data of applicants are handled by the employer for the purpose of realizing the procedure of hiring workforce (to judge aptitude, to prepare for possible employment or to settle potential legal disputes). The purpose ceases to exist when the procedure is finished, then the data have to be deleted pursuant to Point c) of Paragraph (1) of Article 14 of the Act on Data Protection. In practice it means that the purpose for which the data are controlled will not cease until the final deadline of initiating legal disputes possibly arising from the decision reached, therefore they do not have to be deleted. However, as no legal dispute concerning the interview can be expected after the period specified in relevant rules of law has passed, the data have to be deleted *(570/K/2002).*[23]

Several complaints were against the employers' violations in handling various personal identification numbers; some objected to being asked to supply their personal identification code. The Data Protection Commissioner pointed out that employers had no right to control the personal identification

[23] Ombudsman 2002 report, http://www.obh.hu/adatved/magyar/2002/tart1.htm

code, because they were neither authorized by law nor did they fulfil a task specified by law that would require them to do so.

c) There were some complaints by job candidates and employees who objected to the wide scope of information demanded from them as part of various aptitude tests. Citizens in clerical positions protested against the fact that some of the data taken down by the occupational physician on a form were irrelevant to deciding aptitude for their job descriptions. As the grounds for processing the data, the employers identified a Decree of the Ministry of Welfare [33/1998 (VI.24)] on the medical examination and evaluation of job-related, professional and personal aptitude. Paragraph 1(a) of this regulation defines the occupational aptitude test as the examination of whether the person is able to handle the stress entailed by the specific job description in the given workplace. Paragraph 4(1)(a) requires advance occupational aptitude testing of job applicants prior to hiring. The petitioners took the test as required by the Decree, some at the time of their appointment, others a week or two later, by filling out the form supplied in Annex 13 of the Decree under the title "*Employee Medical Record Sheet.*" The physician relayed to the employer a synopsis only, but did keep a record of the detailed health data obtained.

The rules of purposefulness allow that ascertaining aptitude for a job is a legitimate objective of controlling medical and personal identification data [Section 4(1)(n)], but – at the same time – they prohibit the use of these data in excess of what is strictly necessary to accomplish the legally defined purpose of the processing [Section 4(4)]. The Decree requires the collection of a wide range of information in defiance of these principles, and the Record Sheet contained several types of data the knowledge of which was unnecessary for the purpose of deciding aptitude for most jobs. These included information on cardio-vascular, respiratory, tumorous, digestive, metabolic and psychiatric conditions of parents and siblings; smoking and drinking habits (type, quantity, year of quitting); exercise and eating habits; as well as data related to drivers licence, military service, dental health, and a host of other details. Many of the data could be relevant to some jobs and irrelevant to others.

In summary, the Data Commissioner concluded that the provision of the Decree requiring aptitude tests before hiring was not in itself antithetical to the protection of personal data, but the collection of data for the test prescribed in that particular form certainly was. To begin with, the Record Sheet disregarded the principle of purposefulness by demanding a wide range of data from employees, in most cases including information about third persons or otherwise irrelevant for the purpose at hand. In addition, the administrative Decree was not of sufficient rank in the chain of statutory instruments.

d) In another case the data protection commissioner gave opinion about the security data sheet to be filled in by employees in confidential posts; according to this opinion such data handling can be lawful only if the requirements

necessary for taking certain posts are defined in advance as well as the data on the basis of which it can be decided whether the applicant is suitable for taking the post. If the data sheet contains other persons' data, for example data of the family members, the consent of each person concerned has to be obtained. The registered data have to be stored in accordance with the requirements of data security as long as it is necessary. The commissioner disapproved of questions in the data sheet concerning the spouse's income, children, parents, brothers and sisters, previous income and previous criminal cases and offences. According to his order the data had to be preserved for five years even if the employment relationship was terminated. (228/A/2000)

In accordance with the rules of the act on data protection the consent of the person concerned is necessary for handling personal and special data; in the case of special data a written consent is necessary. However, there is one restriction even in the case of the consent of the person concerned: such data can be handled only for a definite purpose, in order to exercise a right and fulfil an obligation, and only to the extent and for the duration necessary for realising the purpose. (§ 5 of the Act on Data Protection).

If the person concerned does not get the job, the data have to be destroyed, or the data sheet and other data obtained during the control have to be handed over to him or her. During the period of data handling the data controller is obliged to give information to the person concerned, which information has to contain the elements listed in Paragraph (1) of Article 12 of the Act on Data Protection.[24]

3. Protection of personal rights during the existence of employment relationship

During the existence of the employment relationship the infringement of personality rights is typically encountered in connection with the supervision and observation of employees. According to the effective act on data protection, the supervision is not unlawful if the employee agrees to it.[25] The most common forms of supervision – for example, observing work with cameras, personal searching and checking of the employees' bags, controlling of telephone and computer use – can be applied only if the employee gives consent. The consent may be of individual nature or may be stipulated in the labour contract, in which the forms of control may also be laid down. It is very

[24] Paragraph 12 (1) of the Act on Data Protection: "Data controller shall inform the data subject, at his or her request, of the processing of his or her personal data performed either by the data controller or by a data processor, the purpose of the processing, its legal basis and duration, the name and address and activity in connection with the data processing of a data processor, as well as of who received or will receive data and for what purpose."

[25] This notion has become superseded in the legal rules and legal practice of the European Union.

important that no employee may suffer disadvantage for not giving consent to control. (For example, if in the case of theft, the employer wishes to search the employees immediately on the spot.)

An increasing number of employers use biometric means for identification or entrance (these use the measurable physical properties of the users). In connection with this the commissioner pointed out that physical properties serving as the basis of identification (for example fingerprint, retina or iris picture, geometry of the hand, characteristics of the voice and face) are personal data for the handling of which the employer has no statutory authorisation, therefore they can be handled only with the consent of the persons concerned. The commissioner informed the petitioners about the conditions of the lawfulness of these systems and pointed out that there is no legal obstacle to their introduction, but at the same time their usefulness or practical applicability may be doubtful on account of the guarantees to be given. (658/K/2000, 832/K/2000)

3.1. Observation of employees with a camera

The only general rule with respect to this is that if the employees do not give consent to being observed in such a way, a camera system should be used in the pictures of which the persons concerned cannot be recognised, so the employees cannot be identified on the basis of the pictures. The employees have to be informed about the setting up of cameras beforehand and whether the pictures will be registered and stored, and if so, for what purpose. If the pictures are registered in every case without restrictions, it is against the act on data protection. Cameras can be used only for a specific purpose, use against this purpose is unlawful. The persons concerned are entitled to see the pictures made about them and may also request the erasure of registerings.

3.2. Control of the use of the workplace telephone

The employer is not entitled to check telephone use by listing telephone calls. The fact that two persons were engaged in a telephone conversation with each other qualifies as personal data both for the caller and the person called. Therefore it qualifies as personal data that an employee called a given number and it is similarly personal data that the person called is in some form of relationship with the caller. As it is practically impossible to obtain the consent of the person called, telephone call listings would be unlawful even if the employees gave their consent. However, there are other ways for reducing the costs lawfully. One possible solution is to prohibit private telephone conversations or to place public telephones (operating with coins or a telephone card) in the workplace. Another solution – also popular with employees – is that the possibility to telephone is provided for the employees up to a certain

sum, the amount determined is higher than the estimated cost of official telephone calls, the value of private calls allowed for the employees is added to it, it is a "present" from the employer to the employees. It is easier to estimate the sum of official telephone conversations if long distance calls in Hungary or to abroad can be made only from certain telephones. The cost of telephone conversations over the sum determined in this way is to be paid by the employee.

Occasionally employers start senseless data collection. Their employees are requested to supply data whose purpose of controlling is inscrutable. In a given case an employee reported that in his workplace not only was the use of their own mobile phones forbidden but they were not even allowed to take the switched-off phones to their workplace. Although the Data Commissioner's competence did not extend to this injury, he could take a standing in connection with the employer's measure according to which the employers had to hand over not only their mobile phone numbers but also the list of calls made from them. In some occupations where employees have to be on call the employer may need the telephone number and if the employee hands it over voluntarily, the employer is entitled to control it. At the same time in the Data Commissioner's opinion no purpose is imaginable for which the employer would need the data of calls made from the employee's own telephone, therefore the request for such data is obviously against the principle of specified purpose. *(429/A/2002)*

In another case the driving licence number and passport number was asked from each employee in a workplace independently of their job. Persons refusing to supply such data were told that it was not compulsory to work there. According to the Data Commissioner this data controlling was also against the principle of specified purpose. *(174/A/2002)*[26]

3.3. Protection of the secrecy of correspondence

In connection with the protection of the secrecy of correspondence the data protection commissioner stated that the protection of the secrecy of correspondence is due to the citizens in their workplace, too. This statement also applies to employees in public administration. Two very important interests have to be manifested in the correspondence and filing order of organs of public administration: one is that the right to the secrecy of correspondence has to be ensured for the addressees of private letters, the other is that the official filing and secret protection of official letters – including qualified ones – also has to be provided.

The file handling regulation of ministries and public administration organs with national competence was laid down by the Government in the Government

[26] Ombudsman 2002 report, http://www.obh.hu/adatved/magyar/2002/tart1.htm

Decree of 40/1998. (III. 6.). Not only the opening of letters "into one's own hand" but that of definitely private letters with personal addressing is also prohibited by the legal rule. The criteria of determining private nature are not detailed by the Government Decree. The judgement of this depends on local characteristics and experiences, too. Chapter IV of the Government Decree states that "on the mistaken opening of the letter, or if it turns out later that the letter contains a qualified document, the envelope shall be closed again, the name of the opening person shall be written on it, then the letter shall be forwarded urgently to the addressee together with the register taken, or the qualified document shall be sent to the file handler. The fact of receipt and opening as well as the date of receipt are to be included in the delivery receipt book by the opening person."

In view of the fact that several regulations did not meet the requirements of the Government Decree, the commissioner proposed that if there is doubt about definitely private-nature letters arriving at the office, it should be opened by the addressee for reasons of guarantee to see whether the letter is private or official, whether it has to be filed or not. He also proposed to the Ministry of Health that the staff of the Ministry should be informed in a circular that if they engage in private correspondence under the Ministry's address, the sender should be asked to indicate "into one's own hand" on the envelope. If the sender fails to do this and if the clerk wanting to open and to file the letter thinks that the letter is "definitely private, with a personal addressing", the addressee himself or herself should open the letter. (791/K/1998)

Personality rights are also affected if the alcoholic state of the employee is checked by a breathalyser, or more recently if the employee is subjected to a drug test, which is also possible according to judicial practice – if it is applied without abuse.

3.4. Checking of workplace computers, e-mail and Internet use

There were several inquiries, on the phone and in writing, about whether employers had the right to access the employees' electronic correspondence and web site visits using computers at the workplace. In one case it was asked the Commissioner to reply by e-mail, as a way of notifying the employer in case he happened to monitor the employee's mailbox illegally.

If the computer was given by the employer for personal use, the employer cannot get to know the personal data stored on it without the consent of the person concerned. Naturally, if the employee gives back the computer to the employer, he or she has to delete private files if he or she does not want the new owner of the computer to know these files; otherwise it is regarded as if he or she had given consent to get to know the data as he or she gave them to the employer personally.

As concerns electronic correspondence provided by the employer, a distinction has to be made between e-mail addresses for the personal use of the employee, possibly containing his or her name or part of his or here name and e-mail addresses which are for managing the company's matters and are not attached to the employee's person. The employer is entitled to have a look at the correspondence under the latter address even if private correspondence was also conducted under this address by an employee – who had access to this post box – as the employee was fully aware of this. Correspondence under a private e-mail address to which only the employee concerned (and the system manager) has access has to be considered, from the aspect of data protection, as traditional personal correspondence and telephoning. Just as the employer is not entitled to know the contents of letters mailed to the employee under the company's address without the consent of the person concerned, or to hold them back, to destroy them or to tap telephone conversations, similarly it is not entitled to know the contents of letters arriving at or sent from a private e-mail address, to forward them or to delete them without the consent of the person concerned.

The nature of Internet pages visited and the frequency of visiting them qualifies as personal data. A distinction has to be made whether the employer permits Internet use exclusively for purposes of work or private use is also allowed. In case Internet use is permitted by the employer only for the purpose of work, the employer is entitled to check this. However, it can do so only if the employees' attention was drawn previously to the restriction of Internet use and to the possibility of subsequent control. If the employees have access to Internet without receiving such information before – or if the employer definitely consented to private use – data concerning Internet use, the pages visited cannot be known by the employer. Should he check Internet use and make a report or have a report made about this, it qualifies as unlawful data handling.

Complaints in connection with monitoring telephone, Internet and e-mail use at the workplace are typical. In 2002 a petitioner called attention to a surprising phenomenon. Instead of an e-mail message sent to him by a friend to his workplace he received the following e-mail: *"You have received a message which you cannot get on account of its content."* From this he concluded that his employer checks and even censors the content of the letters received by the employees, and the receipt of the letters are sometimes prevented. The investigation started in response to the petition found that the system withheld only letters with program, image and sound file attachments suspected to have viruses. In such cases the addressee is notified and if he or she requests the letter to be forwarded, it will be delivered invariably after virus killing. The Data Commissioner found this practice lawful but considered the above notification misunderstandable so he proposed to make it more informative. *(660/A/2002)*

Petitions related to the data controlling practice of employers rarely concern rules of data safety, but let us see such a case all the same. The petitioner wrote that in the computer network set up in his workplace he, through negligence, reached a site which he did not have the right to visit according to the management of the institution, and for this reason his employer wished to take sanctions against him. The Data Commissioner expounded that in accordance with § 10 of the Act on Data Protection the employer, as data controller, was obliged ensure data security and to take the technical and organizational measures and to develop the procedures which are necessary for the enforcement of this Act and other rules of data and secrecy. Thus the employer has to ensure that no unauthorized person can have access to data and information to be protected within the network. If the employer fails to take these measures, it cannot hold anybody responsible for having access to them as a result of the lack of such measures. If the system protected with an entrance code contains further data to be protected from unathorized access, their protection has to be ensured separately, too. *(102/A/2002)*[27]

3.5. Conflict of interest

Some of the complaints concerned agencies of the administration which made it mandatory for civil servants to state their additional sources of income and business interests. Pursuant to Act XXIII of 1992 on the Legal Status of Civil Servants (the "CSA") the employer's permission is required for a civil servant to enter into further employment and other legal relations – except for certain fields such as science, education, art, proof-reading, editing, and intellectual activity falling under copyright laws. The CSA also prohibits, with certain exceptions, civil servants from serving on the board of directors or supervisors of any business organization, and makes it mandatory for them to disclose in writing any conflict of interest as it may arise. In light of these facts, there was nothing wrong with requiring a statement of no conflict from an applicant for a civil service position. Subsequent to hiring, however, it was no longer up to the employer or supervisor to examine the employee in this regard. Instead, it was the civil servant's responsibility to report any conflict of interest, in the awareness that failure to do so might entail disciplinary action. In short, any other employment, with some exceptions, had to be reported and was subject to the public employer's permission. There was no obligation to report the exempt occupations as long as these did not interfere with the employee's job performance as civil servant, or even a member's share in a company, since these alone were no reason to assume a conflict of interest.

In another case, similar in subject matter without concerning civil servants, a person filed a complaint against the Chief Financial Officer ("CFO") who

[27] Ombudsman 2002 report http://www.obh.hu/adatved/magyar/2002/tart1.htm

required employees to make a written statement of family ties and ties of friendship among each other, as well as with service providers and contractors working for the company. The cover sheet enclosed with the form featured the following notice: *"Providing untruthful information may entail termination of employment."* Upon the intervention of the Commissioner, the CFO was called to task for threatening termination. The executive's reply also revealed that the idea of requiring the statement had originated from the German owner who claimed to have *"uncovered abuses that were assisted by precisely such acquaintances and family ties."* The statements were subsequently forwarded to Germany. The Commissioner concluded that the violation consisted not simply in the intimidation of the employees but also in the collection, storage and cross-border transfer of the data themselves. No employer had the right to make such a statement mandatory for employees. The company committed further violations by not informing the employees of who would process their data and for what purpose. The Commissioner urged the executive to discontinue the illegal control of the employees' data.

3.6. False employer's opinion

The evaluation of the employee's work in the framework of employment relationship, the judgement of his or her qualification and abilities necessary for fulfilling the post, the judgement of his or her human behaviour related to work is the employer's right and task. Generally, the employer is entitled to define what requirements have to be met by its employees, workers, and to what extent the employee, subordinate or worker meets these requirements (Central Court of Pest, Civil Council 70 405/1974). During its decision it exercises its rights ensuing from employment relationship, but this exercise of rights cannot be arbitrary; what is more, it cannot infringe the employee's personal rights beyond the rules of labour law. The exercising of employer's rights belongs to the framework of employment relationship only as long as it does not infringe the employee's other rights – protected (also) by civil law. In case personality rights are infringed, the employee can seek legal remedy according to the rules of civil law, independently of the employment relationship.

Personality rights can be infringed by any statement, evaluation, qualification or description concerning the employee if it damages or insults good reputation or honour irrespective of whether it is expressed in writing, orally or by implied conduct. A misleading or untrue statement concerning the employee's person qualifies as the violation of personality even if it was made during the exercising of employer's rights. Illegal evaluation concerning a person's work or behaviour associated with work infringes not only labour law rules but also personality rights protected by civil law. Proof has to be supplied by the person who puts forward facts, gives opinion or qualification damaging

somebody else's good reputation (Supreme Court, Civil Council I. 20 610/1977).

An untrue or misleading statement, evaluation, description or qualification in connection with employment relationship means damage of reputation, therefore the possibility of using means for personality protection opens in civil law.

Damage of reputation can take the form of hidden hints, allusions and concealment, too. Infringement of rights is realised by means of concealment if the qualification contains only facts unfavourable for the employee while favourable facts and aspects essential for the qualified person's judgement are concealed. In the judgement of an unlawful statement concerning employment relationship it is of no importance what the source of the untrue facts is. With respect to ascertaining infringement of rights the imputation of the employer's conduct and whether it is in good or bad faith need not be examined, and the directly detectable consequences need not be proved, either.

The employee's personality rights can also be infringed by means of humiliating or rough treatment. This is the case, for example, when the work performed by the employee is disparaged and belittled by the employer without due grounds. In this case the employee is entitled to give in his or her extraordinary notice according to Point b) of Paragraph (1) of Article 96 of the Labour Code, which states that: *"Employment relationship can be terminated with extraordinary notice by the employer or by the employee if the other party' conduct makes the maintaining of employment relationship impossible.(...)"*

In this case the employee cannot be expected to maintain employment relationship. Moreover, on account of the infringement of his or her personality rights he or she can enforce his or her claim on the basis of the Civil Code, too. Personality rights can also be infringed by the use of the so-called "disgrace board", by making the violation of the obligation on the employee's part public. There is no possibility for this in a lawful manner – used as a detrimental legal consequence. Moreover, according to Paragraph (2) of Article 109 : *"The collective bargaining agreement can specify only such disadvantages associated with employment relationship as detrimental legal consequences which do not infringe the employee's personality rights and human dignity. (...)"*

Needless to say, not every evaluation, description or criticism concerning the employee qualifies as infringement of rights just because it does not suit the employee's interests. For example: the workers of the defendant company informed their superior that they were unable to work with the plaintiff as the plaintiff's behaviour was unbearable, rebuking, commanding and condescending towards her colleagues, she could not fit in with the community. The witnesses in the lawsuit also testified that the plaintiff treated her colleagues in a condescending and commanding manner, she tended to cry and

shout, and for this reason they did not wish to work with her. Thus by claiming that the plaintiff had difficulties in fitting in with the community, the defendant gave true information and thus the plaintiff's personality rights were not infringed (Budapest Higher Court, Civil Council 20 237/1987)

No infringement of rights occurs, either, if only the evaluating part of the statement or qualification – for example the opinion concerning the employee's aptitude for work, leadership qualities – is mistaken. This infringement can be remedied only within the scope of labour law, if at all. A labour law suit cannot be filed claiming that the employer – possibly mistakenly – considers somebody unsuitable for leadership and for this reason his or her application is refused. However, the qualification infringes rights if the worker was declared by the employer to be unsuitable for filling a managerial post on the basis of untrue facts. (Veszprém District Court P 20 137/1974)

In the case of personality infringement associated with the exercising of employer's rights (untrue opinion, untruthful qualification, employer's qualification insulting the employee) the offender in fact acts in the employer's name. The employer is responsible for his or her behaviour. This responsibility is objective as the activity is of a representative nature. The employer also has to take responsibility if the employee acting on behalf of the employer exceeded his or her scope of activities.

The infringement of personality rights associated with employment relationship can also arise after the termination of the employment relationship. Supplying data and evaluation by the former employer (information, opinion, description, judgement) can infringe personality rights; this is the case if the supplied data and the evaluation can be insulting and damage reputation.

4. Assertion of rights

Personality rights can be asserted in a civil procedure against persons handling personal data unlawfully, the data controller can be taken to court. In the lawsuit compensation for possibly arising damage – pecuniary and non-pecuniary – can be claimed. The latter one can be claimed if the human personality's physical or mental life quality has changed unfavourably in consequence of infringing personality rights. The court in the place of the controller's business shall have jurisdiction over the case. The data controller is obliged to prove in the lawsuit that data handling corresponds to the legal regulations, so in this case the general rule of the obligation to produce evidence does not apply – according to this the plaintiff would have to prove the statements made in the lawsuit (that is the statement that his or her data were handled unlawfully by the data controller). In addition to this possibility of assertion of right, the data protection commissioner's help may also be requested.

Summary

The Hungarian data protection law belongs to a quite advanced generation of this family of legal documents, not so much for the technical execution of its language as for its conceptual framework and philosophy. In this connection it is needed to point out four distinctive features. Hungarian law: *a)* essentially disregards the physical attributes of the data subject, making no distinction between data controlled by traditional methods and by computers; *b)* lumps various data controllers together as a general category (that is to say, it holds citizens worthy of protection equally from administrative power, civilian organisations, business organisations, the press and other citizens); *c)* works with a system of concepts which complies with European standards; and *d)* finally (and while this feature is immaterial from the aspect of European legal harmonisation, it is all the more noteworthy in view of international trends), the Hungarian Data Protection Act is unique in Europe in that it is not really an act of "data protection," as it is habitually referred to, but rather a law on rights to freedom of information. As such, it governs not only the protection of personal data but also the guarantees of freedom of information, entrusting these two rights to the same protection, to the Commissioner for Data Protection and Freedom of Information.

The working legal models most akin to the Hungarian way are to be found in North America.

Perhaps the most obvious structural weakness of Hungarian data protection law is the low level of self-regulation, which is clearly one of the most important areas in the everyday life and legal practice. The self-regulation of data protection means the systematic rules set up independently, but with regard to national law by professions, associations, bodies, chambers and the business sector. Self-regulation imparts vigour and an organic character to the progress of data protection. The EU Data Protection Directive discusses self-regulation as one of the pillars of data protection, both on the national and the European level. "The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the various sectors." Beyond encouragement, the Directive also recommends that professional associations – as the data controllers – submit their regulations to the data protection authority in order to check that they indeed comply with the national data protection law and thus with the Directive itself. It is the area of self-regulation in which Hungarian data protection law clearly falls behind European Union standards.

Bibliography

BEDDARD, DR. RALPH: *Human Rights and Europe*, Third Edition, Cambridge, Grotius Publications Limited, 1993.

Condition of work digest, Worker's privacy Part I: Protection of personal data, Volume 10, No. 2, ILO, Geneva, 1991.

Condition of work digest, Worker's privacy Part II: Monitoring and surveillance in the workplace, Volume 12, No. 1, ILO, Geneva, 1993.

Condition of work digest, Worker's privacy Part III: Testing in the workplace, Volume 12, No. 2, ILO, Geneva, 1993.

DIETZ GUSZTÁVNÉ DR. PAP MÁRTA: *Adatvédelem, adatbiztonság* (Data protection, data safety); Novorg Kiadó, Budapest, 1995.

DUSTON, ROBERT L.; RUSSEL, KAREN S.; SHEPARD, MICHAEL: *Workplace Privacy.* Washington D.C.,1989.

Employee Relations Law Journal, Vol.24(3) Winter 1998.

European Union Review, IDS Employment Europe 458 Febr. 2000.

DR. FABÓK ANDRÁS: A munkavállaló személyiségi jogainak és személyes adatainak védelme (The protection of employees' privacy and personal data), In: *Munkaügyi Szemle*, 4/2000, 39-41.p.

F. HATHÓ KATALIN: *Adatbiztonság, adatvédelem* (Data protection, data safety); Számalk Kiadó, Budapest, 2001.

FINKIN, W. MATTHEW: *Privacy in Employment Law*; BNA Books, The Bureau of National Affairs, Inc., Washington, D.C., USA, 1996.

GOLD, MICHAEL, EVAN: *An Introduction to the Law of Employment Discrimination.* ILR

HAYDEN, TRUDY; HENDRIKS, EVAN; NOVIK, JACK D.: *Your Right to Privacy*, Southern Illinois Univ. Press, Carbondale, 1990.

HORVÁTH TIBOR, KERESZTY BÉLA, MARÁZ VILMOSNÉ, NAGY FERENC, VIDA MIHÁLY: *A magyar büntetőjog különös része* (Hungarian Criminal Law); Korona Kiadó, Budapest, 1999.

IDS Employment Europe 457 January 2000

Legal Issues of European Intergration 1996/1, Kluwer Law International Legal issues of European integration 1992/1, Kluwer Law and Taxation Publishers

DR. MAJTÉNYI LÁSZLÓ: *Az adatvédelem Magyarországon és az Európai Unióban* (Data protection in Hungary and in the European Union); Kiadó: Magyar Posta Rt., Budapest, 1999.

MCWHIRTER, DARIEN A.: *Your Rights at Work.* John Wiley and Sons, Inc., 1993.

MICHAEL SHEPARD – ROBERT L. DUSTON – KAREN S. RUSSELL: *Workplace Privacy; Employee testing, surveillance, wrongful discharge and other areas of vulnerability.* The Bureau of National Affairs, Inc. Washington DC. 1989.

NEAL,ALAN C.: *European Labour Law and Social Policy* (Cases and Materials) Kluwer Law International,1999.

Petrik Ferenc, szerk.: *A személyiség jogi védelme* (Privacy protection), KJK, Budapest, 1992.

DR. RYTKÓ EMÍLIA, DR. BELÁNSZKI GYULA: *Nyilvántartási rendszerek és adatvédelem* (Data registration systems and data protection); Magyar Közigazgatási Intézet, Budapest, 2001.

SÁRI JÁNOS: *Alapjogok /Alkotmánytan II./* (Basic rights /Constitutional Law II./), Osiris Kiadó, Budapest, 2001.

SÓLYOM LÁSZLÓ: A személyiségi jogok elmélete (Theory of personal rights); KJK, Budapest, 1983.

Transfer European Review of Labour and Research, Vol. 5(3) Autumn, 1999.

WACKS, RAYMOND: *Personal Information, Privacy and the Law*. Oxford,1989.

The Hungarian Constitutional Court Decision No. 15/1991. (IV.13.)

Ombudsman 1999 report, http://www.obh.hu/adatved

Ombudsman 2000 report, http://www.obh.hu/adatved

Ombudsman 2001 report, http://www.obh.hu/adatved

Ombudsman 2002 report, http://www.obh.hu/adatved

HAJDÚ JÓZSEF

A MUNKAVÁLLALÓK SZEMÉLYISÉGI JOGÁNAK VÉDELME MAGYARORSZÁGON, KÜLÖNÖS TEKINTETTEL AZ ADATVÉDELEMRE

(Összefoglalás)

Az emberi érintkezés egyik legfontosabb és leggyakoribb színtere a munkahely, a munkavégzés. A személyiségi jogok sérelmének veszélye itt fokozottabban fennáll. Magyarországon – különösen a rendszerváltást követően – a munkavállalók alárendelt helyzete, alultájékozottsága, öntudathiánya és a technikai fejlődés eredményeként lehetővé váló adatgyűjtés és adatfeldolgozás is hozzájárult ahhoz, hogy a munkavállalók személyiségi jogai folyamatosan veszélyben vannak.

Magyarországon a 90-es évek elejétől egyre nagyobb mértékben nő a munkavállalók munkaerőpiaci függősége, kiszolgáltatottsága. A korábban kivívott – noha gyakran kiüresedett – munkavállalói jogok folyamatos erodálódása, rosszabb érvényesíthetősége, a munkahelyi érdekképviseletek visszaszorulása figyelhető meg. Az információs hatalom túlsúlya a munkáltató oldalán, a munkavállaló oldalán gyakran létrejövő hátrányos, egyenlőtlen kommunikációs helyzet sérti az alapvető személyhez fűződő jogokat és a magánszféra sérthetetlenségét (right to privacy).

A fenti kontextusba ágyazva a dolgozat két részből tevődik össze. Az elsőben a magyar adatvédelmi törvény szabályozásának legfontosabb sajátosságait vázoltuk fel. A másodikban pedig a munkavállalók személyiségi jogait védő jogi szabályozás struktúráját mutattuk be. A jobb megértés érdekében az elméleti megközelítés mellett a második részben néhány fontosabb példát és jogesetet emeltünk ki a magyar Adatvédelmi Biztos és a különböző szintű bíróságok gyakorlatából.